ABSTRACT:

The invention relates to a method for authenticating a first unit to a second unit and, in particular, to a method for transmitting data securely over a transmission channel from a security unit to an application unit. Known data transmission methods and systems use a revocation list stored in a security unit, e. g. in a CD drive, listing identifiers of revoked application units. In order to provide an environment for secure transmission of encrypted data and/or keys where the data and/or the keys are protected against copying, hacking and other misuse and which requires only a minimum storage capacity in the security unit a method for authenticating a first unit to a second unit is proposed according to the invention comprising the steps of:

a) exchanging authentication data between said first unit and said second unit, said authentication data being retrieved from an authorisation list comprising a list identifier, and

b) checking the authenticity of the authorisation list and the origin of the authentication data from a valid authorisation list.

Fig. 3